==========

H I P A A L E R T Volume 2 No. 9 July 11, 2001

>> From Phoenix Health Systems...HIPAA Knowledge...HIPAA Solutions <<
> Healthcare IT Consulting & Outsourcing <

==========

HIPAAlert is published monthly in support of the healthcare industry's efforts to work together towards HIPAA security and privacy. Direct subscribers total 12500+!

Do you have interested associates? They can subscribe free at: http://www.hipaadvisory.com/alert/

IF YOU LIKE HIPAALERT, YOU'LL LOVE HIPAADVISORY.COM! -- Phoenix' comprehensive "HIPAA hub of the Internet," per Modern Healthcare magazine. Visit: http://www.hipaadvisory.com

==========

T H I S I S S U E

==========

1 / F R O M T H E E D I T O R S:

Some industry observers feared that DHHS' promised Privacy Rule Guidance communications would be a shot in the dark, but the first Guidance has relieved many by at least partially hitting the mark. Common sense and practicality have prevailed -- sound-proof rooms and encrypted phone conversations are not required by HIPAA. Providers aren't "marketing" when describing their services, and friends and relatives can pick up a patient's prescription at the

pharmacy. This Guidance doesn't cover the field by any means -- we'll need more clarification on business associates, minimum necessary uses and disclosures, parents and minors, and government access. From all appearances though, DHHS is readying more salvos in the form of new Guidance and Privacy Rule modifications later this year....

In the meantime, our detailed point-by-point overview of the first Guidance follows. For HIPAAprivacy "newbies" we've also provided a new summary of the overall Privacy rule. HIPAAnews reports on the latest privacy breach that is causing Eli Lilly to draw fire, and in HIPAAdvisor, Steve Fox and Rachel Wilson address how HIPAA and Faxing work together.

If you haven't yet discovered our new HIPAAstore on HIPAAdvisory.com, stop by for a browse. By popular demand -- yours! -- we now offer HIPAA compliance audioconferences, tapes and books -- with more to come.

Diane Boettcher, Editor
dboettcher@phoenixhealth.com

D'Arcy Guerin Gue, Publisher
daggue@phoenixhealth.com

PS. DON'T MISS - HIMSS' Flash Audioconference dissecting the First Privacy Guidance this Friday afternoon. The program, co-sponsored by Phoenix Health Systems, and presented by Phoenix Principal and HIPAA expert Helene Guilfoy, will offer a solid hour of succinct analysis and live Q/A on this important new HIPAA development.
Friday, 1 pm Central Time.
To register, go to
http://www.himss.org/templates/ContentRedirector.asp?ContentId=4443

==========

2 /THE PRIVACY RULE: DHHS' First Guidance Missile
By D'Arcy Guerin Gue, Executive Vice President, Knowledge Services and Business Development, Phoenix Health Systems

On July 6, 2001 the Department of Health and Human Services issued the first of "several technical assistance" materials it has promised on the HIPAA Privacy Rule. The stated purposes of this Guidance: to

clarify the Privacy Rule's provisions and reflect DHHS' intent not to interfere with patients' access to healthcare or to the quality of healthcare.

The Department plans to offer future guidance and to issue proposed modifications "expeditiously...to correct any unintended negative effects." Modifications to the Privacy Rule require publishing them in the Federal Register through the Notice of Proposed Rulemaking (NPRM) process and providing for public comment before issuing a final rule. In the meantime, DHHS is preparing Guidance clarifications so that the industry may begin implementing the Privacy Rule to meet its April 14, 2003 compliance date.

OVERVIEW

The Guidance reaffirms that the Privacy Rule is needed because the protections provided by "the old system of paper records in locked file cabinets is not enough...under the current patchwork of laws, personal health information can be distributed -- without either notice or consent -- for reasons that have nothing to do with a patient's medical treatment or health care reimbursement."

Scalable compliance options are emphasized throughout the Guidance; it reiterates that providers and payers have flexibility to create their own privacy procedures, and that these procedures may be "tailored to fit their size and needs."

LIKELY RULE CHANGES / MODIFICATIONS TO BE PROPOSED

- Pharmacists may fill physicians' phone-in prescriptions before obtaining patient consent.

- Providers to whom a patient has been referred for the first time, can use personal health info to set up appointments or schedule procedures.

- Covered entities may engage in whatever communications are necessary for "quick, effective, high quality healthcare" including routine oral communications with family and staff.

- Common practices such as sign-up sheets, X-ray light boards and bedside medical charts are not prohibited.

- Possible changes to ensure parents have appropriate access to information about the health of their children

---

WHO IS COVERED?

The Guidance notes that health plans, clearinghouses, and providers who conduct electronic transactions electronically are covered even if their "business associates" perform some essential functions for them. Though DHHS has no authority to govern entities who are not healthplans, clearinghouses or healthcare providers, it can and does require them to have contracts outlining specific provisions, with business associates.

CONSENT

DHHS reaffirms that the Privacy Rule builds on customary health practices rather than replacing them. With its consent provisions, it sets "a uniform standard for certain health care providers to obtain patient consent for uses and disclosures of health information" to carry out treatment, payment or healthcare operations (TPO). The Rule does not limit -- or intend to address -- consent for treatment. Its focus is on ACCESS to health information, not the underlying treatment. Clarifications include:

- Consent is not required in an emergency, when law requires treatment, or when there are substantial communications barriers, but must be obtained as soon as reasonably practicable.

- Providers with indirect treatment relationships (i.e., laboratories, who only interact with the physician and not the patient health plans and clearinghouses) may use and disclose personal health info for purposes of TPO without getting consent.

- Consulting with another provider -- another indirect relationship -- does not require the other provider to obtain consent.

- Providers can refuse treatment if a patient refuses consent for use or disclosure of his personal information to carry out the treatment, payment or healthcare operations.

- Providers need to obtain the patient's written consent only once, whether there is a "connected course of treatment" or treatment for unrelated conditions -- and aren't required to verify a signature if the patient isn't present.

- A patient may revoke consent in writing, but this excludes actions already taken in reliance on the consent. The patient can also

request restrictions on uses and disclosures; the covered entity doesn't have to agree, but is bound by anything it does agree to. The caregiver may bill and expect payment for care provided after obtaining consent, even if the patient revokes consent.

- Certain integrated organizations, including an organized healthcare arrangement located in different states, may rely on one joint consent for all.

- Providers can rely on consents received before the compliance deadline of April 14, 2003 for use and disclosure of information received before that date.

- Pharmacists may give advice on over-the-counter medicines as long as this is just a conversation, and no records of personal information are set up.

- Pharmacists can make "reasonable inferences" about the patient's best interest to allow someone other than the patient to pick up a prescription. This includes family and friends.

- If a provider believes that waiting for patient consent would compromise patient care, he can use or disclose personal health information for emergency treatment. Patient consent must be sought as soon thereafter as is reasonable.

MINIMUM NECESSARY

The "minimum necessary" use and disclosure of personal health information to accomplish the intended purpose does NOT apply to:

- Disclosures to providers for treatment purposes.
- Disclosures to the patient himself.
- Uses or disclosures for which an individual has signed an authorization.
- Uses or disclosures required to comply with HIPAA transactions.
- Disclosures to DHHS that are needed in order to enforce HIPAA.
- Uses or disclosures that are required by other law.

For routine disclosures, covered entities may rely on policies and procedures as standard protocols if they define "minimum necessary" for staff to carry out their jobs. If it's non-routine, a disclosure must be reviewed individually using reasonable criteria.

Covered entities may rely on the requesting party’s judgment on the minimum necessary, if the request is "reasonable" and if made by public officials for certain legal or public health purposes, another covered

entity, a professional staff member or business associate, or a researcher who has received appropriate documentation from his review board. However, the covered entity instead may use its own discretion to make the determination.

DHHS plans to modify the Privacy rule to increase confidence that covered entities are "free to engage in whatever communications are required for quick, high quality care."

Covered entities are required to assess for themselves what personal health information is necessary to achieve a particular purpose. However, this does not necessarily require uses and disclosures to be limited only to information "that is absolutely necessary". The Guidance clarifies that the standard is a "reasonableness" standard, not a strict one -- which enables a best practices approach consistent with existing professional standards.

The Guidance also confirms that the covered entity is in the best position to "know and determine who in its workforce needs access" to personal health information, including entire medical records, for treatment purposes -- and recommends that providers develop role-based access policies.

If an entity believes that a request is for more than the minimum necessary information to achieve the intended purpose, the disclosing entity must make the final determination. But if an individual authorizes disclosure of his information to third parties such as government agencies, life insurers and others, the entity does not have to make any minimum necessary determination. However, the entity must make this determination if it has requested the authorization for its own purposes.

The Guidance emphasizes the scalability of compliance with the minimum necessary provision, pointing out that "reasonable efforts" are required to limit access to personal health information. What is reasonable for a paper-based organization with three or four staff compared to a complex hospital environment is likely to be very different. For example, in the former, it may not be practical to limit certain employees' access to parts of the patient record, but a large organization with electronic patient records systems very likely may need to establish limited access fields. Similarly, organizations are expected to take reasonable precautions against exposing bedside charts, prescription vials and X-ray light boards to the public; they are not required to eliminate them or totally isolate them from all functions.

The Guidance admits that the Privacy Rule is "ambiguous" about the use of sign-in sheets in physician offices and other similar practices.

Modifications will be developed indicating that these customary practices are permitted.

ORAL COMMUNICATIONS

DHHS emphasizes that oral communications must be covered by the Privacy Rule because if they were not, any health information could be available to anyone, as long as it was spoken. The Privacy Rule doesn't wish to keep providers from talking to each other -- nor does it require eliminating all risk of prohibited disclosures. Customary practices such as speaking loudly in a crowded emergency room, discussing patients over the phone, coordinating services orally at a nursing station, and discussing a patient's condition during training rounds are permissible, with "reasonable precautions" such as standing apart and lowering voices. Similarly, structural changes such as soundproofing, private rooms or encryption of phone systems, aren't necessary. A suggested alternative solution is providing curtains, screens or cubicles in areas where multiple patient-staff discussions take place.

The Rule does not require recording oral conversations involving patients' health information. However, if conversations have been recorded and then used in decision-making about the patient, individuals may have access to these records. Nor does the Rule require documenting any information, including oral, that is used or disclosed for treatment, payment or healthcare operations. If disclosures are made for other purposes, such as disclosure of a health condition to a public health agency, they must be documented as part of the patient's disclosure history.

BUSINESS ASSOCIATES

A central Privacy Rule tenet is reaffirmed, that personal health information may be disclosed to a business associates only to help providers and plans complete their healthcare functions. Business associates may not use the information in any other way.

- Members of a provider, health plan or other covered entity's workforce are not considered business associates. Nor are covered entities who exchange personal health information for treatment purposes, such as a physician who discloses information to a hospital where he has admitting privileges.

- The Privacy Rule doesn't "pass through" its requirements to business associates; it has no authority to do so. Covered entities must obtain assurances from their business associates that they

will use the information only for the purposes that they were engaged to perform, will safeguard the information from misuse and will help the entity comply with its HIPAA obligations. Typically this agreement will be accomplished by contract between the covered entity and the business partner. Covered entities are not liable for privacy violations of a business associate. However, if they become aware of a "pattern or practice" that is a material breach of the business associate's contract, they must take "reasonable steps" to correct the problem. If unsuccessful, they may have to terminate the contract or report the problem to DHHS. Only if the covered entity doesn't take these steps would it be considered non-compliant with the Rule.

PARENTS AND MINORS

A parent or guardian is considered the "personal representative" of his or her minor child, and has the right to see the child's personal health information. There are a few exceptions:

- If a minor consents to services where a state or other law doesn't require parental consent, the parent is no longer considered the personal representative.

- When a parent agrees to a confidential relationship between the child and the physician, he or she may not have access to the child's health information.

- If a covered entity believes that the child is an abuse or neglect victim, or may be endangered by the parent, the entity may choose not to treat the parent as the child's personal representative. In these cases, parents do not have the right to see their children's medical records.

The Guidance notes that Secretary Thompson is reassessing these provisions to ensure "that parents have appropriate access to information about the health and well-being of their children."

MARKETING

The Privacy Rule limits how personal health information may be used in marketing, including the kind of marketing that may be done as a part of healthcare operation. Marketing is defined as communicating about a product or service in order to encourage its purchase or use.

Certain activities that otherwise meet this definition, are NOT considered marketing under the Privacy Rule "to prevent interference

with essential treatment or health-related communications with a patient." They include:

- Describing participating providers or plans in a network -- or the services and benefits they provide.

- Using the communication to provide, manage or further treatment -- as in recommending over-the-counter medications or sending reminder notices for appointments or prescription refills.

If a communication IS marketing, personal health information may be used or disclosed only in these cases:

- Face-to-face encounters with the patient -- as in offering product samples during an office visit.

- They involve products or services of nominal value, i.e., toothbrushes, pens, etc.

- They concern health-related products and services of the covered entity or a third party, and if the covered entity making communication is identified.

- It is stated that the covered entity is being paid for the communication, if this is so.

- The individuals are told how to opt out of further marketing

- Individual are told why they have been targeted (Are they diabetics, smokers?) and how the communication relates to their health.

- They are marketing-related disclosures made to business associates only to support the covered entity's marketing activities. The entity must require a signed business associate agreement from its telemarketer or door-to-door salesman, who may not use protected health information for his own or other purposes.

Under the Privacy Rule, all other marketing requires individual authorizations to use or disclose personal health information. In order to release patient or enrollee lists for any other reasons, the covered entity must obtain authorization from everyone on the list.

RESEARCH

Covered entities may use and disclose personal health information for health research with authorization by individual participants -- or

without it under limited circumstances:

- The covered entity must be notified that the appropriate Review Board has approved waiver or alteration of authorization. An example might be records research, in which it is impractical to find participants and obtain authorization.

- The researcher uses the information only to prepare a necessary research protocol or similar document, and will not remove any personal health information.

- The research is only on decedents, the personal health information is necessary, and the deaths of the individuals can be documented.

The Guidance argues that requiring individual authorization for certain research and limiting unauthorized research as described above will not hinder medical advances. It suggests that patients will be more willing to participate if their information is protected, and cites a National Institutes of Health (NIH) study in which over 30% of eligible participants declined a test for breast cancer for fear of insurance discrimination.

GOVERNMENT ACCESS

The only new authority the Privacy Rule provides for government is in its enforcement role of the Privacy Rule itself. The Office of Civil Rights (OCR) has the right to receive enough information to investigate complaints and ensure compliance. Otherwise, government health providers and healthplans such as Medicare and Medicaid have to meet essentially the same requirements as private organizations. The Guidance also confirms that the Rule does not require physicians or others to send medical information to the government for a databases or similar reason.

Police and other law enforcement access to information also is not expanded by the Rule. According to the Guidance, access will be more limited than provided currently. Law enforcers will not receive DNA information without a warrant; and entities must get permission from victims of domestic abuse before disclosing their information.

PAYMENT

The Privacy Rule allows "payment" to include disclosures to consumer reporting agencies, but these are limited to basic non-health information such as name, social security number, date of birth and payment history.

Covered entities may use collection agencies through a business associate agreement. In general, DHHS maintains that there is no conflict between the Rule and the Fair Credit Reporting act or the Debt Collection Practices Act.

For the full text of the Privacy Guidance of July 6, 2001, go to:
http://www.hipaadvisory.com/regs/finalprivacy/guidance.htm

Questions are being taken by DHHS at:
http://www.hhs.gov/ocr/hipaa2.html

==========

3 /HIPAAprivacy: A Privacy Primer

Official Name: Standards for Privacy of Individually Identifiable Health Information (45 CFR Parts 160 through 164)

Current Status: Final rule published December 28, 2000; became effective April 14, 2001

BACKGROUND AND PURPOSE OF THE RULE

The HIPAA Privacy rule is the first federal law to take a comprehensive approach to protecting the privacy of personal health information. When HIPAA mandated standardization of electronic healthcare transactions, it also included language requiring safeguards to protect the privacy and security of that information. The law gave Congress until August 21, 1999 to develop and pass health privacy legislation, but Congress failed to do so. Since HIPAA required the Department of Health and Human Services (DHHS) to promulgate its own health privacy regulations in this event, DHHS proposed a Privacy rule (NPRM) in November 1999. Following a lengthy process of public comment and re-drafting, the final Privacy rule was published on December 28, 2000. The Secretary of DHHS announced that the law would take effect on April 14, 2001, despite strong controversy within the healthcare industry regarding the potential costs and difficulties of compliance.

WHO IS COVERED?

The Privacy rule applies to all health plans and healthcare clearinghouses. The rule also covers all healthcare providers who electronically transmit personal health information in connection with

the transactions for which HIPAA has developed standards. Business associates who use or have access to covered personal health information are indirectly affected via required "Business Associate Agreements."

OVERVIEW OF THE PRIVACY RULE

The Privacy rule reflects several basic principles that underlie HIPAA administrative simplification as a whole. These include:

- Consumers' right to view and control the use and disclosure of their personal health information

- Boundaries that limit use of health information to direct healthcare purposes, unless patients authorize otherwise

- Accountability for violating patients' privacy

- A need for balance between the public's responsibility to support medical research, public health and quality of care, and the need for personal health information privacy

- Ensuring the security of personal health information

KEY PROVISIONS

- The privacy rule protects all individually identifiable health information that is used or disclosed by covered entities, regardless of whether it is in electronic, paper or oral form. Information that has been de-identified is not covered.

- Covered entities are required to educate patients in writing on the privacy protections employed when storing, using and disclosing their health information.

- Patients must be allowed to view and receive copies of their health records. They must also be able to request amendments to their records, and to receive a history of disclosures of their information. (Disclosure is defined as disclosures outside of the covered entity.)

- With some exceptions, patient consent must be received before personal information is used for purposes of treatment, payment or healthcare operations.

- With some exceptions, authorization by the patient is required for

uses and disclosures of personal information for purposes other than treatment, payment or healthcare operations.

- Uses and disclosures other than those between providers for treatment purposes may not exceed the minimum amount of information necessary to accomplish the intended purpose, unless they are disclosed within a standard transaction.

- Every covered entity must designate a privacy official responsible for developing and implementing privacy policies and procedures.

- Business associate agreements must be executed with third parties to whom protected health information is disclosed or made available for purposes of performing services or functions for the covered entity.

- The Privacy rule preempts State laws when they are less stringent than the federal law. The Privacy rule is intended to set a national "floor" of privacy standards; if states have enacted stronger privacy measures, the federal law does not preempt them.

EFFECTIVE DATES

For most healthcare providers, clearinghouses and healthplans, compliance with the Privacy rule is required by April 14, 2003. Small healthplans who have annual receipts of $5 million or less have an additional 12 months to comply; their deadline is April 14, 2004.

==========

*** Drug Maker's Privacy Breach Reveals Patient E-mail Addresses ***

Pharmaceutical maker, Eli Lilly, blamed a programming error for a June 27th incident in which it accidentally disclosed the e-mail addresses of about 600 medical patients to each other. An electronic message was sent to registered users of a "reminder" service, according to company spokeswoman Anne Griffin. But all of their e-mail addresses were revealed in the message's "to" field, instead of just each individual's address, she said.

Analysts said the mistake points to the need for health care organizations to assess whether the way they communicate with patients violates HIPAA medical data privacy rules. The ACLU has

called for an investigation for possible violation of federal trade laws.

For more information, go to:
http://www.hipaadvisory.com/news/index.htm#stan0705

*** AHA Reacts to Privacy Guidance ***

The AHA welcomed DHHS' issuance of its first HIPAA privacy regs guidance, but said critical issues still need to be addressed. The association said DHHS appears to have taken steps toward assisting hospitals in such key areas as minimum necessary standards, oral communications and consent requirements. However, AHA said the guidance does not address concerns on issues such as data aggregation for benchmarking, business associate requirements, and disclosures to the government.

For more information, go to:
http://www.hipaadvisory.com/news/index.htm#aha0710

*** NCVHS Offers New HIPAA Recommendations to DHHS ***

The National Committee on Vital and Health Statistics (NCVHS) has recommended to DHHS Secretary Thompson a number of steps to help hospitals implement HIPAA. NCVHS recommended that DHHS supply early guidance on implementation of the standards, allow flexibility in enforcing them and should not allow a delay in the implementation date.

NCVHS Chairman John Lumpkin, M.D., and Director of the Illinois Department of Public Health, delivered these and other recommendations, in a letter to Thompson on June 29th.

For the full text of the letter, go to:
http://www.hipaadvisory.com/news/2001/ncvhsltr0629.htm

*** EMR Rule May Be Released Next Year ***

DHHS has indicated it will release a Proposed Rule (NPRM) for Electronic Medical Records (EMR) Standards, probably during the second quarter of 2002. HIPAA mandated that DHHS "study the issues related to the adoption of uniform data standards for patient medical record information (PMRI) and the electronic exchange of

such information."

For more information, go to:
http://www.hipaadvisory.com/news/index.htm#hl0627

==========

5 / H I P A A d v i s o r : Legal Q/A with Steve Fox, Esq.

*** Just the Fax Facts ***

QUESTION: Can you offer guidance about sending and receiving faxes that contain individually identifiable patient information? Are fax transmissions covered under HIPAA's privacy standards or do the security standards govern these transactions?

ANSWER: The proposed security standards and the privacy standards both set forth requirements designed to protect the confidentiality and privacy of certain health information. Therefore, covered entities will be required to comply with both of these rules whenever they send or receive fax transmissions containing individually identifiable health information, also referred to as protected health information ("PHI").

Essentially, the privacy standards identify and define exactly what type of information is protected and in what context such information may be used and/or disclosed. In contrast, the proposed security standards establish a framework for executing those disclosures permitted under the privacy standards.

The question being asked requires an examination of the means by which covered entities will maintain the confidentiality of PHI. Accordingly, this discussion revolves around the proposed security standards (the "security standards").

The security standards apply to PHI that is either electronically maintained or transmitted. These standards require covered entities to implement:

1. administrative procedures, physical safeguards, and technical security services to guard data integrity, confidentiality, and availability and

2. technical security mechanisms to prevent unauthorized access to data that is transmitted over a communications network. Following are some

examples of procedures and safeguards that covered entities may want to implement in order to protect the security of fax transmissions:

ADMINISTRATIVE PROCEDURES

- Train staff to double check the recipient's fax number before transmittal and to confirm delivery via telephone or review of the appropriate confirmation of fax transmittal.
- Include a pre-printed confidentiality statement on all fax cover sheets. The statement should instruct the receiver to destroy the faxed materials and contact the sender immediately, in the event that the transmission reached him/her in error.

PHYSICAL SAFEGUARDS & TECHNICAL SECURITY MECHANISMS

- Place fax machines in areas that require security keys, badges, or similar mechanisms in order to gain access.
- Periodically remind regular fax recipients to provide notification in the event that their fax number changes.

TECHNICAL SECURITY SERVICES

- Make certain that audit controls, like fax transmittal summaries and confirmation sheets are stored and reviewed periodically for unauthorized access or use.
- Pre-program and test destination numbers in order to minimize the potential for human error.

Remember, security measures cannot be implemented in a vacuum. It order to be successful, covered entities will need to fully integrate the security standards into their strategies for compliance with the privacy standards.

It is also important to keep in mind that although the security standards have not yet been finalized, the original HIPAA law passed by Congress already requires covered entities to "maintain reasonable and appropriate administrative, technical, and physical safeguards" designed to ensure the integrity and confidentiality of PHI, and to protect against any reasonably anticipated:

1. threats to the security or integrity of PHI
2. unauthorized uses or disclosures and
3. ensure compliance with the law by the covered entity's officers and employees.

This article was co-authored by Rachel H. Wilson, an associate at Pepper Hamilton LLP.

To read past HIPAAdvisor articles, go to:
http://www.hipaadvisory.com/action/HIPAAdvisor.htm

Steve Fox, Esq., is a partner at the Washington, D.C. office of Pepper Hamilton LLP. This article was co-authored by Rachel H. Wilson, Esq., an associate at Pepper Hamilton. Pepper Hamilton LLP is a multi-practice law firm with more than 400 lawyers in ten offices.
http://www.pepperlaw.com/

Disclaimer: This information is general in nature and should not be relied upon as legal advice. Only your attorney is qualified to evaluate your specific situation and provide you with customized advice.

==========
COMMENTS? Email us at info@phoenixhealth.com
SUBSCRIBE? Visit http://www.hipaadvisory.com/alert/
ARCHIVES: http://www.hipaadvisory.com/alert/newsarchives.htm
==========

http://www.phoenixhealth.com 301-869-7300
==========

FORWARD this posting to interested associates, who may subscribe free to HIPAAlert at:
http://www.hipaadvisory.com/alert/
Subscribe to our free discussion list at:
http://www.hipaadvisory.com/live/
Get a weekly byte of HIPAA at:
http://www.hipaadvisory.com/notes/

You are currently subscribed to hipaalert as:kmckinst@dmhhq.state.ca.us
To unsubscribe send a blank email to leave-hipaalert-8507990O@lists.hipaalert.com